#3

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT

Applicant(s): Philip D. MacKenzie
Case: 9
Serial No.: 09/827,227
Filing Date: April 5, 2001
Group: TBA

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS/SUBCLASS	FILING DATE IF APPROPRIATE
MV	5,440,635	08/08/95	Bellovin et al.		
	5,241,599	08/31/93	Bellovin et al.		
	09/638,320	08/14/00	V.V. Boyko et al., "Secure Mutual Network Authentication and Key Exchange Protocol."		
	09/353,468	07/13/99	P.D. MacKenzie et al., "Secure Mutual Network Authentication Protocol (SNAPI)."		

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	COUNTRY	CLASS/SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS

EXAMINER INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
MV		1. D. Jablon, "Strong Password-Only Authenticated Key Exchange," ACM Computer Communications Review, ACM SIGCOMM, pp. 1-22, 1996.
		2. S.M. Bellovin et al., "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.
		3. S.M. Bellovin et al., "Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise," Proceedings of the First Annual Conference on Computer and Communications Security, pages 1-7, 1993.
		4. M. Steiner et al., "Refinement and Extension of Encrypted Key Exchange," ACM Operating System Review, pp. 1-9, 1994.
		5. T. Wu, "The Secure Remote Password Protocol," Proceedings of the 1998 Internet Society Symposium on Network and Distributed System Security, pages 1-17, 1997.
		6. Stefan Lucks, "Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys," Security Protocol Workshop, pp. 1-12, 1997.
		7. M. Bellare et al., "Authenticated Key Exchange Secure Against Dictionary Attacks," Advances in Cryptology, pp. 1-16, Eurocrypt 2000.

Examiner Michael Vaughan — Date Considered 4-7-04

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

#3

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT

Applicant(s): Philip D. MacKenzie
Case: 9
Serial No.: 09/827,227
Filing Date: April 5, 2001
Group: TBA

OTHER DOCUMENTS-(Cont'd)

EXAMINER INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
MV	8.	S. Patel, "Number Theoretic Attacks on Secure Password Schemes," Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 236-247, 1997.
	9.	W. Diffie et al., "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT 22, No. 6, pp. 644-654, 1976.
	10.	FIPS 180-1, "Secure Hash Standard," Federal Information Processing Standards Publication 180-1, pp. 1-21, 1995.
	11.	H. Dobbertin et al., RIPEMD-160: a Strengthened Version of RIPEMD, Fast Software Encryption, 3rd Intl. Workshop, pp. 1-13, 1996.
	12.	R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.
MV	13.	D.P. Jablon, "Extended Password Key Exchange Protocols Immune to Dictionary Attack," WETICE Workshop on Enterprise Security, pp. 1-8, 1997.

Examiner Michael Vaughan Date Considered 4-7-04

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT

Applicant(s): Philip D. MacKenzie
Case: 9
Serial No.: 09/827,227
Filing Date: April 5, 2001
Group: 2131

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS/SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	COUNTRY	CLASS/SUBCLASS	TRANSLATION YES	TRANSLATION NO
MV	EP 1 134 929 A1	09/19/01	Europe			

OTHER DOCUMENTS

EXAMINER INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
MV		V. Boyko et al., "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," Advances in Cryptology, Eurocrypt 2000, pp. 156-171, 2000.

Examiner Michael Vaughan

Date Considered 4-7-04

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.